UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/727,158	12/02/2003	Simon Robert Walmsley	PEA24US	6703

24011 7590 07/01/2008

SILVERBROOK RESEARCH PTY LTD
393 DARLING STREET
BALMAIN, 2041
AUSTRALIA

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	PAPER NUMBER
2134	
MAIL DATE	DELIVERY MODE
07/01/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/727,158	WALMSLEY, SIMON ROBERT	
	Examiner	Art Unit	
	ANDREW L. NALVEN	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *5/8/08*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18 and 20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18 and 20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-18 and 20 are pending.

Response to Arguments

2. Applicant's remaining arguments filed 5/8/08 have been fully considered but they are moot in view of the new grounds of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. **Claims 1-3, 5, and 7-17 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Mi et al US PGPub 2002/0116616 in view of Wiener US Patent No. 7,273,483 and Shiell et al US Patent No. 6,065,113.

4. **With regards to claim 1**, Mi teaches determining a method of manufacturing a series of integrated circuits having related functionality, the method including the steps of determining an identifier (Mi, paragraph 0021, processor number), permanently storing the identifier on one of the integrated circuits (Mi, paragraph 0021, stored in a

constant ROM or processor ID register), repeated steps (a) and (b) for each integrated circuit in the series (Mi, paragraph 0021, more than one device has processor number), wherein the identifiers for the series are determined in such a way that knowing the identifier of one of the integrated circuits does not improve the ability of an attacker to determine the identifier of any of the other integrated circuits (Mi, paragraph 0021, statistically unique for a given processor). Mi fails to teach the unique identifier being 64 bits or implemented by selectively blowing 224 bits of fuses. However, Weiner teaches the unique identifier being 64 bits (Weiner, column 13 lines 24-49, 64 bit). Further, Shiell teaches selectively blowing fuses in a number greater than the number of identifier bits in order to provide error correction (Shiell, column 5 line 60 – column 6 line 30, claim 13). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Weiner's method of using 64 bit identifiers and Shiell's method of blowing fuses because it offers the advantage of being large enough to allow for unique identification and give information regarding compatibility and usability (Weiner, column 13 lines 24-49) and because it helps provide error correction abilities when reading bits from fuses to ensure that an incorrect identifier is not read (Shiell, column 5 line 60 – column 6 line 30).

5. **With regards to claim 2**, Mi as modified teaches the identifier for each integrated circuit is determined using a stochastic mechanism thereby rending highly improbably that replication of some or all of the series of identifiers stored on the series of the integrated circuits (Mi, paragraph 0021, statistically unique).

6. **With regards to claim 3**, Mi as modified teaches each of the integrated circuits incorporates an identifier determined and stored in accordance with claim 1 (Mi, paragraph 0021, more than one device has processor number).

7. **With regards to claim 5**, Mi as modified teaches the integrated circuit operable in a first and second mode (Mi, paragraph 0042, authorized or unauthorized state), wherein in the first mode, supervisor code can access the identifier (Mi, paragraphs 0042-0043, applets that are verified and authorized can access processor number) and in the second mode, user code cannot access the identifier (Mi, paragraphs 0042-0043, applets that are not verified and not authorized cannot access processor number).

8. **With regards to claim 7**, Mi as modified teaches the identifier mapped into a key K (Mi, paragraph 0024, identifier mapped into XOR result of identifier-211 and secret key).

9. **With regards to claim 8,** Mi as modified teaches that K is the identifier (Mi, paragraph 0021, processor number).

10. **With regards to claim 9**, Mi as modified teaches K is created by applying a hash function or one-way function to the identifier (Mi, paragraph 0024, identifier is hashed using SHA-1 or MD5).

11. **With regards to claim 10**, Mi as modified teaches the integrated circuit configured to produce and output a message from the integrated circuit (Mi, paragraph 0030, client computer sends return value to server) the message including a result of encrypting K (Mi, paragraph 0030, paragraph 0031, paragraph 0024, second XOR on intermediate value-K using session identifier).

12. **With regards to claim 11**, Mi as modified teaches injecting a key into a target integrated circuit (Mi, paragraph 0030, server receives return value) comprising the step of receiving the message generated by the first integrated circuit of claim 10, and transferring a second key into the target integrated circuit (Mi, paragraph 0030, server receives return value), the second key being based on K (Mi, paragraph 0024, second XOR on intermediate value-K using session identifier).

13. **With regards to claim 12**, Mi as modified teaches generating the second key by manipulating K with a function (Mi, paragraph 0024, K manipulated using second XOR function).

14. **With regards to claim 13**, Mi as modified teaches the function uses K and a code associated with the target integrated circuit as operands (Mi, paragraph 0024, function uses K and session identifier associated with session between client and server).

15. **With regards to claim 14,** Mi as modified teaches that the code is a code that is relatively unique to the target integrated circuit (Mi, paragraph 0023).

16. **With regards to claim 15,** Mi as modified teaches K and the second key enabling secure communication between the first integrated circuit and the target integrated circuit (Mi, paragraph 0031, K and return value-second key are used by server to determine if access is permitted, paragraph 0036).

17. **With regards to claim 16**, Mi as modified teaches the second integrated circuit configured to communicate securely with a third integrated circuit (Mi, paragraphs 0052-0054, web server communicates with those seeking to participate in a teleconference),

thereby enabling it to act as an intermediary between the first integrated circuit and the third integrated circuit (Mi, paragraphs 0052-0054, web server acts as intermediary between members of the teleconference) allowing secure communication there between (Mi, paragraph 0055).

18. **With regards to claim 17**, Mi as modified teaches the first and third integrated circuits do not share a key for use in the secure communication (Mi, paragraph 0061, web server acts as a gatekeeper).

19. **Claims 4, 18, and 20 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Mi et al US PGPub 2002/0116616, Shiell et al US Patent No. 6,065,113 and Wiener US Patent No. 7,273,483, as applied to claim 1 above, and in further view of Debry US Patent No. 6,314,521.

20. **With regards to claim 4**, Mi fails to teach the integrated circuits being printer controllers. However, Debry teaches each integrated circuit being a printer controller (Debry, column 8 lines 18-29, unique encryption key embedded in each manufactured printer). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Debry's method of placing unique identifiers within printer controllers because it offers the advantage of allowing a printer to be able to prove to a sender that it is the actual printer device that the printer purports to be (Debry, column 5 lines 65-67, column 6 lines 4-11).

21. **With regards to claim 18**, Mi teaches a first integrated circuit configured to perform an authenticated read of a third integrated circuit by securely communicating via the second integrated circuit (Mi, paragraph 0061, server forwards identifiers), but

fails to teach the first integrated circuit being a print controller. However, Debry teaches an integrated circuit being a printer controller (Debry, column 8 lines 18-29, unique encryption key embedded in each manufactured printer). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Debry's method of placing unique identifiers within printer controllers because it offers the advantage of allowing a printer to be able to prove to a sender that it is the actual printer device that the printer purports to be (Debry, column 5 lines 65-67, column 6 lines 4-11).

22. **With regards to claim 20**, Mi as modified teaches the authenticated read relating to monitoring or updating usage of a resource (Debry, column 8 lines 18-30 and 53-56, printer is updated with digital certificate).

23. **Claim 6 is rejected under 35 U.S.C. 103(a)** as being unpatentable over Mi et al US PGPub 2002/0116616, Shiell et al US Patent No. 6,065,113 and Wiener US Patent No. 7,273,483, as applied to claim 1 above, and in further view of Collins et al US Patent No. 7,055,029.

24. **With regards to claim 6,** Mi fails to teach the supervisor mode being available to a program upon verification of that program by a boot program of the integrated circuit. However, Collins teaches teach the supervisor mode being available to a program upon verification of that program by a boot program of the integrated circuit (Collins, column 5 lines 7-15, column 9 line 65 – column 10 line 17, control of processor is transferred to black-boot program upon verification). At the time the invention was made, it would

have been obvious to a person of ordinary skill in the art to utilize Collin's method of verifying program using a boot program because it offers the advantage of ensuring the security of the computer system itself and of all processes handled by the computer system (Collins, column 2 lines 40-49).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANDREW L. NALVEN whose telephone number is (571)272-3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Andrew L Nalven/
Primary Examiner, Art Unit 2134